Zyxel lanza parche para vulnerabilidad crítica de inyección de comandos del sistema operativo de firewall

Autor: I. Stepanenko

Fecha: Friday 27th of May 2022 12:27:26 PM

Zyxel abordó una vulnerabilidad de seguridad crítica que afecta a los dispositivos de firewall Zyxel, que permite a los hackers remotos y no autenticados obtener la ejecución de código arbitrario.

> «Una vulnerabilidad de inyección de comandos en el programa CGI de algunas versiones de firewall podría permitir que un atacante modifique archivos específicos y luego ejecute algunos comandos del sistema operativo en un dispositivo vulnerable», dijo la compañía.

La firma de seguridad cibernética Rapid7, que descubrió e informó la vulnerabilidad el 13 de abril de 2022, dijo que la debilidad podría permitir que un adversario remoto no autenticado ejecute código como el usuario *«nobody»* en los dispositivos afectados.

Rastreada como CVE-2022-30525 con puntuación CVSS de 9.8, la vulnerabilidad afecta a los siguientes productos, con parches lanzados en la versión ZLD V5.30:

USG FLEX 100 (An), 200, 500, 700
USG FLEX 50(W)/USG20(W)-VPN
Serie ATP
Serie VPN
Rapid7 dijo que hay al menos 16,213 dispositivos Zyxel vulnerables expuestos a Internet, lo que lo convierte en un lucrativo vector de ataque para que los atacantes realicen posibles intentos de explotación.

La compañía de ciberseguridad también dijo que Zyxel emitió silenciosamente correcciones para abordar el problema el 28 de abril de 2022, sin publicar un identificador de vulnerabilidades y exposiciones comunes (CVE) asociado o un aviso de seguridad. Zyxel culpó sobre esto en su alerta a una *«falta de comunicación durante el proceso de coordinación de divulgación».*

Zyxel lanza parche para vulnerabilidad crítica de inyección de comandos del sistema operativo de firewall

Autor: I. Stepanenko

Fecha: Friday 27th of May 2022 12:27:26 PM

> «El parcheo silencioso de vulnerabilidades tiende a ayudar solo a los atacantes activos y deja a los defensores en la oscuridad sobre el verdadero riesgo de los problemas recién descubiertos», dijo Jake Baines, investigador de Rapid7.

El aviso se produce cuando Zyxel abordó tres problemas distintos, incluyendo una inyección de comando (CVE-2022-26413), un desbordamiento de búfer (CVE-2022-26414) y una falla de escalada de privilegios locales (CVE-2022-0556), en su VMG3313, Router inalámbrico T20A y configurador de AP que podría conducir a la ejecución de código arbitrario.